TP4
Configuration IPsec entre deux machines Linux

1 Objectif

Sécurisation d'une communication host-to-host par le biais du IPsec en mode "transport"

2 L'IPsec - Internet Protocol Security

IPsec (Internet Protocol Security), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques, est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme et c'est la raison pour laquelle il est considéré comme un cadre de standards ouverts. De plus IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IPsec[1].

3 Plateforme du TP

Pour la réalisation de ce tp, on va adopter la plateforme illustrée au schéma suivant:

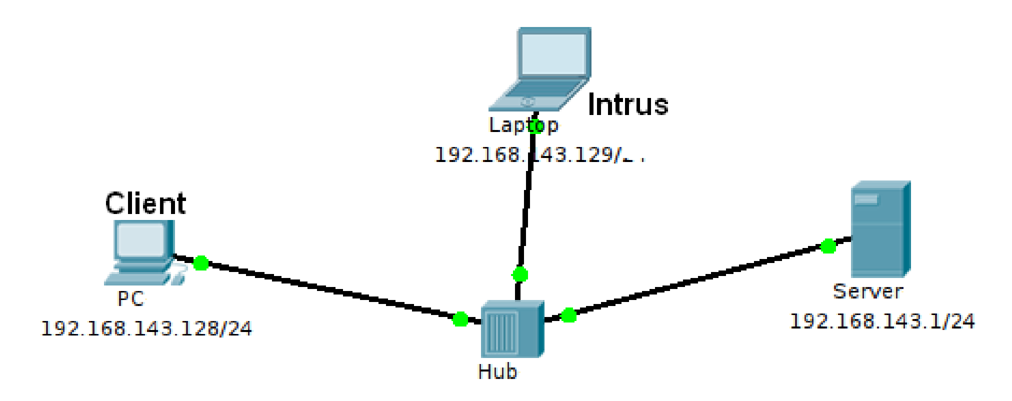


Figure 1: Réseau LAN

4 Configuration des SAs et des SPDs de la machine 192.168.15.130

- Éditez en mode superutilisateur le fichier /etc/ipsectools.conf (en annexe à ce TP)
- Dans ce fichier, seront configurés les SAs et les SPDs qui concernent la liaison qu'on veut sécuriser
- *Lignes 6, 7* Le script commence par nettoyer la SAD et la SPD
- *Lignes 13, 14* Créature de le première SA

  La commande "ADD" ajoute une nouvelle SA

  On définit l'adresse IP source et destination

  On spécifie le protocole (AH ou ESP)

[1]Wikipédia

On identifie notre SA par un indice SPI

On spécifie l'algorithme à utiliser

On indique la clé

- Linux supporte les algorithmes suivants:

  hmac-md5 et hmac-sha pour le hachage (afin d'assurer l'authentification)

  des-cbc and 3des-cbc pour le chiffrement (afin d'assurer la confidentialité)

- *Lignes 25,26,27* Créature de la première SP

  La commande "SPDADD" ajoute une nouvelle politique de sécurité (une politique définit quels paquets devront être protégés)

  On indique les adresses IP source et destination

  On définit le port et la direction du flux

  On décide le sort du flux (ipsec/discard/none)

  On désigne le protocole (ah/esp/ipcomp), le mode (transport/tunnel) et le niveau (use/require)

  Les deux machines doivent avoir les mêmes SAs, la seule différence de leurs fichiers de configuration ipsec réside dans les directions des flux

- Pour prendre en considération la nouvelle configuration, lancez la commande "sudo service setkey start"

- Pour le test, essayez d'écouter le trafic d'une communication icmp par exemple